UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

CAPITOL RECORDS, INC., et al., Plaintiffs, v. NOOR ALAUJAN, Defendant.	Civ. Act. No. 03-cv-11661-NG (LEAD DOCKET NUMBER)

SONY BMG MUSIC ENTERTAINMENT, et al., Plaintiffs, v. JOEL TENENBAUM, Defendant.	Civ. Act. No. 07-cv-11446-NG (ORIGINAL DOCKET NUMBER)

PLAINTIFFS' RESPONSE TO DEFENDANT'S MOTION FOR PROTECTIVE ORDER

Plaintiffs respectfully submit this Response in Opposition to Defendant's Motion for Protective Order, and state as follows:

INTRODUCTION

Plaintiffs request a forensic examination of Defendant's Gateway computer to discover evidence central to their claim for willful and continuous copyright infringement.[1] At the heart of the dispute over Plaintiffs' request is Defendant's counsel's representation that no computer

[1] While Defendant's counsel previously agreed to an inspection of two different computers, in order to streamline these proceedings, Plaintiffs withdraw their request to inspect Defendant's Toshiba computer at this time.

inspection is necessary because there is no computer to inspect.[2] That statement, however, is incorrect. Indeed, Defendant admitted in his deposition that he currently possesses a Gateway computer on which he has installed and used peer to peer software to upload and download sound recordings. The Gateway computer likely has evidence relevant not only to Plaintiffs' allegations as to Defendant's infringement, but also evidence directly relevant to Plaintiffs' allegations of ongoing and willful infringement. As such, the Gateway computer is central to the case. Contrary to Defendant's counsel's assertions, Plaintiffs are not seeking a computer inspection in order to blindly search for documents that may on the computer and may be relevant to case. Here, ***the computer is the very tool used to commit copyright infringement.***

Defendant's Motion should be denied not only because it cites the wrong legal standard and lacks evidentiary support for Defendant's assertions of privilege and confidentiality, but also because Defendant simply does not understand how computer inspections must be done in order to have any integrity. Indeed, it is axiomatic that computer inspections require a mirror image of the entire hard drive both to create a forensically sound copy and to ensure that all data on the hard drive is captured – even deleted files. Moreover, these issues have been litigated in similar cases in the past and, in every instance, the court has ordered the inspection to go forward.

Plaintiffs are not unaware of nor unsympathetic to Defendant's concerns regarding privileged and confidential information. In this respect, Plaintiffs will agree to mechanisms to address these concerns that work within the confines of the technical requirements for a forensic computer examination. Specifically, Plaintiffs propose allowing Defendant to create a privilege log and instructing the third party that conducts the imaging to forensically erase from the mirror imaged hard drive the privileged information before producing it to Plaintiffs. Plaintiffs agree to

[2] Defendant's counsel made this statement to the Court at the September 23, 2008 Status Conference and repeated it in his Motion. *See generally*, Motion.

a similar procedure and limited redaction of confidential information, such as student grades, unpublished research, and medical records. *See* Exhibit A, Plaintiffs' proposed Protective Order.

RELEVANT FACTUAL BACKGROUND

On August 10, 2004, a third-party retained by Plaintiffs, MediaSentry, detected an individual using the KaZaA P2P file sharing system under the username "sublimeguy14@KaZaA" to engage in online copyright infringement. Plaintiffs sent a pre-litigation letter to the individual responsible for the Internet account through which the infringement occurred. Plaintiffs invited the recipient of the letter to contact them to discuss resolution of the case, and in any event, to be certain to preserve all relevant evidence in the case. In response, Defendant contacted Plaintiffs' representatives and identified himself as the target of any claims. After the parties were unable to settle this matter, Plaintiffs filed their Complaint against Defendant on August 7, 2007. In their Complaint, Plaintiffs allege that Defendant willfully and continuously used a P2P system to illegally download and distribute their copyrighted sound recordings. Compl. ¶¶ 13, 15.

On September 23, 2008, Defendant's counsel represented to the Court that no computer inspection was necessary in this case because there was no computer to inspect. On September 24, 2008, Plaintiffs deposed Defendant and learned that this representation to the Court was not accurate. During his deposition, Defendant admitted to using multiple P2P systems on several different computers over the course of many years to download and distribute sound recordings over the Internet. First, Defendant used the original Napster service until it was shut down in 2003. Tenenbaum depo. at 106:24–109:21. After Napster was shut down, Defendant began using KaZaA to download music from the Internet. *Id.* at 107:10-108:13. Specifically, Defendant admits using KaZaA and the "sublimeguy14@KaZaA" username on a computer he

identified as the "no name computer." *Id.* at 31:6-32:21; 81:24-83:17; 98:1-98:21. Defendant testified, however, that the "no name computer" has since been discarded. *Id.* at 98:1-100:4. Similarly, Defendant admits that he used LimeWire, and may have used KaZaA, to download music onto the Gateway computer.[3] *Id.* at 90:20-94:20.

Additionally, when he left for college, Defendant copied "between 50 and 600" sound recordings from his KaZaA shared folder on the "no name computer" onto compact discs ("CDs") and took them with him to college. *Id.* at 209:10-211:18.

In short, Defendant is a serial downloader who used multiple P2P systems over many years to illegally download and distribute sound recordings through the Internet. Defendant, however, conveniently could not recall any of the specifics of his downloading. As such, the Gateway computer, which likely contains evidence of Defendant's willful and continuous downloading, is central to Plaintiffs' claim.

PROCEDURAL HISTORY

On September 29, 2008, Plaintiffs' counsel requested a forensic examination of Defendant's Gateway and Toshiba computers. *See* Decl. of Eve Burton ("Burton Decl."), ¶ 2, Exhibit B. Defendant's counsel responded the next day, agreed to the request, and set a time and location for the mirror imaging of the computers. *Id.*, at ¶ 3. On October 1, 2008, however, Defendant's counsel contacted Plaintiffs' counsel and expressed concern regarding the previously agreed-to imaging. *Id.*, at ¶ 4. Defendant's counsel suggested limiting the imaging to specific portions of the hard drive or allowing Defendant to delete privileged or confidential information before the imaging. *Id.* Plaintiffs' counsel explained that an image of the entire hard drive is necessary to ensure sound evidence. *Id., at* ¶ 5. Moreover, a forensic inspection is

[3] Defendant also admits he may have used KaZaA on the eMachine computer at his parents' house. *Id.* at 88:18-89:1; 100:20-101:20.

the appropriate method to access relevant evidence that may not be searchable by a lay person because it resides in the hard drive's deleted space or in metadata. Plaintiffs' counsel again warned that Defendant should not delete information himself, as such removal must be done forensically to prevent spoliation. *Id.*

To accommodate Defendant's concerns, Plaintiffs proposed a protective order which has been approved in substantially similar form by many courts around the country. *Id.*, at ¶ 6. Under the proposed protective order, the third party imager would redact privileged information before delivering the hard drive to Plaintiffs' expert and private or confidential information would be protected from disclosure. *Id.* On October 2, 2008, Plaintiffs served on Defendant a Rule 34 request and the proposed protective order. *Id.*, at ¶ 7. Defendant's counsel rejected the proposed protective order in a two sentence email and filed a Motion for Protective Order on October 15, 2008. *Id.*, at ¶ 8.

As established below, Defendant's Motion should be denied because the Gateway computer is central to Plaintiffs' claim. Given Defendant's description of his use of the Gateway computer, it is clear that the computer will have on it evidence regarding Defendant's use of peer to peer networks and his infringing behavior. Defendant's unsupported assertion that the computer is not relevant is belied by the facts. And Defendant's unsupported assertions that there are privileged and confidential materials on the computer cannot be used as a shield to prevent discovery of clearly relevant evidence when simple and foolproof mechanisms can be employed to protect Defendant's allegedly privileged and confidential information.

I. THE GATEWAY COMPUTER IS DIRECTLY RELEVANT TO PLAINTIFFS' CLAIM OF WILLFUL AND CONTINUOUS COPYRIGHT INFRINGEMENT.

In determining whether information is discoverable under Rule 26(b)(1), courts consider whether "the information sought appears reasonably calculated to lead to the discovery of

admissible evidence." *Klonoski v. Mahlab*, 156 F.3d 255, 267 (1st Cir. 1998) (citing Fed. R. Civ. P. 26(b)(1)).

Further, Rule 34(a)(1) permits any party to serve on any other party:

> A request to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents .... or to inspect and copy, test, or sample any tangible thing which may constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served.

Rule 34(a)(1) is intended to be broad enough to cover all types of computer-based information. Fed. R. Civ. P. 34(a)(1) (2006 amendments) advisory committee's note. Moreover, a computer forensic inspection may be necessary to capture evidence not obtained during a typical search:

> Computer programs may retain draft language, editorial comments, and other deleted matter . . . in an electronic file but not make them apparent to the reader. Information describing the history, tracking, or management of an electronic file (sometimes called "metadata") is usually not apparent to the reader viewing a hard copy or a screen image.

Fed. R. Civ. P. 26(f) (2006 amendments) advisory committee's note.

Not only is computer evidence discoverable where the information sought appears reasonably calculated to lead to the discovery of admissible evidence, but it is often the only method to access deleted files. While it is a well accepted proposition that deleted computer files are discoverable (*see Rowe Entm't, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 427, 431 (S.D.N.Y. 2002)), locating deleted files requires a search of the hard drive rather than the directory utilized by the operating system to show the files to the computer user. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 313 n. 19 (S.D.N.Y. 2003); *see also United States v. Upham*, 168 F.3d 532, 536 (1st Cir. 1999) (previously deleted images can be recovered using specialized utility program).

A. Computer Forensic Exams Are Appropriate Where The Computer Is Central To The Claim.

1. Courts routinely allow forensic computer examinations in similar cases.

Courts look to the relationship between the computer and the wrong that is the subject of the lawsuit to determine if a forensic computer examination is warranted. Where the computer is central to the heart of the claim, forensic examination of the hard drive is appropriate. *See, e.g., Cenveo Corp. v. Slater*, 2007 U.S. Dist. LEXIS 8281, at *4 (E.D. Pa. Jan 31, 2007) (granting computer inspection where defendant used computer equipment and trade secrets to divert customers); *Frees, Inc. v. McMillan*, 2007 U.S. Dist. LEXIS 4343, at*5 (W.D. La. Jan. 22, 2007) (granting Rule 34 request for inspection where computers were most likely place defendant would have downloaded, transmitted, or deposited the pilfered computer data at issue); *Balboa Threadworks, Inc. v. Stucky*, 2006 U.S. Dist. LEXIS 29265 (D. Kan. Mar. 24, 2006) (granting Rule 34 request because the copyright infringement allegedly occurred through the use of the computers); *Ameriwood Indus. v. Liberman*, 2006 U.S. Dist. LEXIS 93380 (E.D. Mo. Dec. 27, 2006) (granting request for computer inspection where central claim was that defendants used the computers "to secrete and distribute plaintiffs' confidential information").

Moreover, courts around the country have granted record company plaintiffs' requests for inspection in similar cases. *Sony BMG Music Entm't v. Arellanes*, 2006 U.S. Dist. LEXIS 7839, at *2 (E.D. Tex. Oct. 27, 2006) (granting inspection and rejecting defendant's proposed restrictions, including neutral expert and search term confirmation); *Arista Records, LLC v. Tschirhart*, Case No. 05-CA03720G, slip. op. (W.D. Tex. Jan. 25, 2006) (attached as Exhibit C); *Atlantic Recording Corp. v. Andersen*, Case No. 05-CV-933-AS (D. Or. July 11, 2006) (attached as Exhibit D) (granting inspection over defendant's objection on privacy grounds); *Sony BMG*

Music Entm't v. Thurmond, Case No. 1:06-cv-01230-DGT-RML, minute order (E.D.N.Y. May 20, 2008); *UMG Recordings, Inc. v. Lindor*, Case No. 1:05-cv-01095-DGT-RML, minute order (E.D.N.Y. Jan. 16, 2008) (granting inspection of peripheral device previously connected to computer). In fact, Plaintiffs are not aware of a single case involving these same claims by similarly situated plaintiffs where a forensic examination has not been allowed.

2. The cases Defendant cites are inapplicable.

The cases Defendant cites in support of his Motion are inapposite. Indeed, these cases might be cited to oppose discovery in a case regarding the sale of physical CDs if Plaintiffs were hoping to find supporting evidence of the sales on the computer. That is not the case at bar. To the contrary, here, Plaintiffs seek to examine the very tool used to commit the infringement. Because none of the cases Defendant cites involve allegations that the computer was used to commit the wrong at issue, or even had a relationship to the claims, they should not be considered. *See, e.g., Hedenburg v. Aramark Am. Food Servs.*, 2007 U.S. Dist. LEXIS 3443 (W.D. Wash. Jan. 17, 2007) (denying inspection where party was "hoping blindly to find something useful in its impeachment of the plaintiff"); *Williams v. Mass. Mut. Life Insur. Co.*, 226 F.R.D. 144 (D. Mass. 2005) (denying inspection where plaintiff was seeking email that he alleged had not been produced in discovery); *Menke v. Broward County Sch. Bd.*, 916 So. 2d 8, 10 (Fla. App. Sept. 25, 2008) (denying request for inspection of defendant and his family's computers in a suit alleging misconduct of a teacher where school board was looking for any emails between teacher and his students); *Bethea v. Comcast*, 218 F.R.D. 328, 330 (D.D.C. 2003) (denying inspection where plaintiff made "no showing that the documents she [sought] actually exist or that the defendant ha[d] unlawfully failed to produce them"). Indeed, each of

these cases involved a fishing expedition by a party looking for documents it alleged were not produced in discovery.

Defendant's remaining cases are not analogous to this case and do not shed light on the appropriateness of a forensic exam here. *See Dikeman v. Stearns*, 253 Ga. App. 646, 647-48 (Ga. App. 2002) (court denied inspection in dispute over legal bills where plaintiff client sued her law firm and sought all hard drives that generated legal documents pertaining to her case); *In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003) (denying plaintiff consumer direct access to the manufacturer's database to conduct searches for related claims); *BG Real Estate Servs., Inc. v. Amer. Equity Insur. Co.*, 2005 U.S. Dist. LEXIS 10330, at *5 (E.D. La. May 18, 2005) (court rejected broadening the scope of discovery to "subject matter discovery" and instead applied the threshold standard of Rule 26(b)(1)).

As established above, the standard is not whether the computer also contains material that is not relevant, but instead whether the computer is reasonably calculated to lead to evidence of the wrong committed. Where, as here, the computer itself is evidence and Defendant and his counsel admit that it may have been used to commit the wrong at issue and likely contains relevant evidence, inspections are warranted. *See* Tenenbaum depo. at 91:11-96:1 (admitting that he may have used KaZaA on the Gateway computer and that he downloaded LimeWire onto the Gateway); Motion at 2 ("most of [the information on Defendant's computer] has no relevance").

B. The Gateway Computer Is Central To Plaintiffs' Claims.

Plaintiffs have alleged that Defendant willfully and continuously used a P2P system to illegally download and distribute their copyrighted sound recordings. Compl. ¶¶ 13, 15. As such, Defendant's peer to peer activities on all computers are relevant. The fact that the Gateway

computer was purchased two years after Defendant's infringing activities were first detected by Plaintiffs in no way forecloses the existence of evidence of illicit downloading, or information related to such downloading, on the computer. *Frees*, 2007 U.S. Dist. LEXIS 4343, at*5 (granting Rule 34 request where computer was purchased two years after the alleged misappropriation). Defendant's recent use of peer to peer software to download and upload sound recordings on the Gateway computer is relevant both to the allegation of willfulness and the allegation of continuous infringement.

1. The Gateway Computer Likely Contains Evidence Of Peer to Peer Usage And The Sound Recordings At Issue.

Plaintiffs expect to find evidence of illegally downloaded sound recordings from Defendant's KaZaA shared folder, which are listed on Exhibit B to the Complaint.[4] First, Defendant testified that he may have used KaZaA on the Gateway computer. Tenenbaum depo. at 91:11- 92:8. Second, Defendant testified that he copied "between 50 and 600" sound recordings from his KaZaA shared folder on the "no name computer" onto CDs when he left for college. *Id.* at 209:10-211:18. As the Gateway is the only computer Defendant had during college, it is the most likely place he would have uploaded, transmitted, or otherwise deposited the transferred sound recordings. *See Frees*, 2007 U.S. Dist. LEXIS 4343, at*5 (granting Rule 34 request where computers were most likely place to find evidence of pilfered data). Indeed, Plaintiffs expect to find not only evidence of the sound recordings Defendant burned onto CDs and took with him to college, but also the metadata associated with those files – the history,

[4] Defendant incorrectly asserts that only the seven sound recordings on Exhibit A to the Complaint are at issue. Motion at 2. To the contrary, the Complaint alleges that Defendant downloaded and distributed certain of the sound recordings listed on Exhibit B. Compl. ¶ 12. It further states that the sound recordings at issue include, but are not limited to, the seven sound recordings on Exhibit A. *Id*. In fact, Plaintiffs have produced copyright registration documents for 31 sound recordings and intend to pursue these recordings at trial. *See* Supplemental Disclosures, including list of recordings at issue, collectively attached as Exhibit E.

tracking, or management of an electronic file. As this metadata is usually not apparent to the reader viewing a hard copy or screen image of electronic files, a forensic computer examination is the only way to capture this evidence. *See Ameriwood*, 2006 U.S. Dist. LEXIS 93380, at *10. Because the "no name computer" has since been discarded, evidence of KaZaA and the sound recordings on the Gateway computer is critical and a forensic examination of the Gateway computer's hard drive may be the only manner of accessing this evidence.

2. The Gateway Computer Likely Contains Evidence Of Continuous, Willful Copyright Infringement.

Even if the Court does not conclude that the forensic computer examination will likely lead to the discovery of admissible evidence of the underlying allegations of infringement in the Complaint, the examination will most definitely lead to the discovery of admissible evidence regarding the allegations that Defendant's conduct was willful and continuous. Under the Copyright Act, willful infringement is that committed with "reckless disregard" for the plaintiff's copyrights. 4-14 Nimmer on Copyright § 14.04; *see also Yurman Design, Inc. v. PAJ, Inc.*, 262 F.3d 101, 112 (2d Cir. 2001) (affirming jury's finding of willful infringement where defendant had been warned of possibility of infringement). Such reckless disregard can be inferred from continuous infringement, a past pattern of infringement, or other circumstances. 4-14 Nimmer on Copyright § 14.04; *Microsoft Corp. v. Evans*, 2007 U.S. Dist. LEXIS 77088, at *15, 18-19 (E.D. Cal. Oct. 16, 2007) (infringement was willful where it was not isolated, but rather was the result of the defendant's continuing involvement in advertising, marketing, installing, and/or distributing the copyrighted materials).

Here, evidence of a subsequently downloaded P2P system and sound recordings is central to Plaintiffs' claim of willful and continuous infringement. During his deposition, Defendant admitted downloading LimeWire onto the Gateway computer and using LimeWire to

download music from the Internet after leaving home for college. Tenenbaum depo. at 92:24-96:1. Defendant conveniently, however, could not recall the specifics regarding his downloading activities. *Id.* at 95:19–96:1. As Defendant could not recall when he started or stopped using LimeWire, or what sound recordings he downloaded using LimeWire, a forensic examination of the Gateway computer's hard drive is the only way to obtain that evidence and determine the extent of his willful and continuous infringement.

Additionally, Plaintiffs require a computer forensic examination to recover any deleted files. As Defendant testified that he probably deleted LimeWire from the Gateway computer, a forensic examination may be the only method of recovering those files. *Id.* at 183:1-5*; Zubulake*, 217 F.R.D. at 313 n. 19; Decl. of Dr. Doug Jacobson, attached hereto as Exhibit F.

As evidence of subsequent infringement goes to the heart of Plaintiffs' claim for willful and continuous copyright infringement, Defendant's Motion should be denied.

III. DEFENDANT HAS NOT BEEN FORTHCOMING IN DISCOVERY.

Defendant's Motion suggests that Defendant has been "forthcoming" in discovery. This is as far from the truth as possible. Recognizing that parties who provide inconsistent and incomplete discovery responses are likely to conceal evidence on their computers, some courts also consider whether a party has been forthcoming in discovery in determining whether to allow computer inspections. *See Calyon v. Mizuho Secs. USA Inc.*, 2007 U.S. Dist. LEXIS 36961, at *10 (S.D.N.Y. May 18, 2008); *Ameriwood*, 2006 U.S. Dist. LEXIS 93380, at *4. In *Ameriwood*, for example, the court explained that "discrepancies or inconsistencies in the responding party's discovery responses may justify a party's request to allow an expert to create and examine a mirror image of a hard drive." 2006 U.S. Dist. LEXIS 93380, at *4 (citation omitted). Similarly, in *Simon Prop. Group L.P. v. MySimon, Inc.*, the court allowed the plaintiff to make mirror

images of the defendant's computers where there were "troubling discrepancies" with respect to the defendant's discovery responses. 194 F.R.D. 639, 641 (S.D. Ind. 2000). While such considerations are unnecessary because in this case the computer is central to the claims at issue, Defendant's conduct during discovery further militates towards allowing the inspection. *See Frees*, 2007 U.S. Dist. LEXIS 4343, at*5.

Here, Defendant provided inaccurate and inconsistent discovery responses and evaded deposition questions. For instance, Defendant first denied all knowledge of Plaintiffs' allegations. Specifically, Defendant denied that an online media distribution system was downloaded to the computer (Response to Request for Admission ("RFA") No. 6), denied knowing that an online media distribution system was downloaded to the computer (Response to RFA No. 7), denied that he used the screen name "sublimeguy14@KaZaA" while connected to an online media distribution system (Response to RFA No. 8), and denied that Exhibit B to the Complaint is or was a copy of his shared folder (Response to RFA No. 9).

Similarly, in his Interrogatory responses, Defendant denied all knowledge of and responsibility for the infringement at issue. First, in identifying all persons who used the computer, Defendant listed a large number of individuals who could have used the computer, including, preposterously, a burglar, but did not list himself. (Response to Interrogatory ("Rog.") No. 7). Next, Defendant claimed to have no knowledge of who used a P2P system (Response to Rog. No. 10) or of any sound recordings which were downloaded onto the computer using a P2P system (Response to Rog. No. 14). Also, Defendant denied knowledge of any screen names used in connection with a P2P system, (Response to Rog. No. 17), and denied knowledge of anyone using the screen name "sublimeguy14@KaZaA." (Response to Rog. No. 18).

Defendant, however, changed his story. First, on September 19, 2008, four days before he finally attended his deposition, Defendant amended his responses to RFA Nos. 6, 7, and 8 to admit that a P2P system was downloaded to the computer, that he knew a P2P system was downloaded to the computer, and that he had used the screen name "sublimeguy14@KaZaA" while connected to a P2P system.[5] *See* August 19, 2008 email, attached as Exhibit G, Discovery requests and responses, Exhibit H.

During his deposition, Defendant provided even more inconsistent responses. For instance, Defendant admitted that he not only used "sublimeguy14@KaZaA" while connected to a P2P system, but that ***he created that screen name***. Tenenbaum depo. at 83:11-13. Similarly, Defendant admitted that Exhibit B to the Complaint was a copy of his shared folder. *Id.* at 268:3-11. Defendant admitted using multiple P2P systems to download sound recordings from the Internet. *Id*. at 92:24–96:1; 106:24–107:7. In fact, he admitted to first using Napster to download music, turning to KaZaA after Napster was shut down for copyright infringement, and finally switching to LimeWire because it had better features. *Id.* at 106:24-112:9; 93:15-19.

Further, Defendant was generally evasive during his deposition.[6] For example, Defendant refused to describe the conversation he had with his mother in response to Plaintiffs' pre-litigation letter.

Q. Did you discuss this case with your mother over the phone?
A. Yes.
. . .
Q. What did your mother say to you?

[5] Defendant twice refused to sit for his properly scheduled deposition. Details can be found in Plaintiffs' September 22, 2008 Status Report. (Doc. No. 657).

[6] Defendant claims that he provided nine hours of sworn testimony. While the deposition ended approximately nine hours after it began, Defendant provided approximately 6 hours of testimony. The remaining time was consumed by breaks, most of which were requested by Defendant's counsel.

A. I don't remember.
Q. Did you discuss the fact that the record companies believed copyright infringement occurred through their Internet account?
A. I believe that question has already been implied through a prior one.
Q. Can you answer it please?
A. As to whether or not my mother and I discussed – I'm sorry. Repeat the question.
MS. GOLDSTEIN BURTON: Can you read it back?
(Question read back.)
A. Yes.
Q. Did you discuss why the record companies might believe that such infringement occurred?
A. I don't remember.
Q. Did you discuss that you may have been responsible for the copyright infringement at issue?
A. Yes.
Q. What did you say?
A. You will have to be more specific.
Q. What did you say to your mother as to who may have been responsible for the copyright infringement at issue that occurred through your parents' Internet account?
A. I said that it was impossible for me to know.
Q. Did she ask you whether you were responsible?
A. I don't remember.
Q. Why did you say it was impossible for you to know?
A. Because it was impossible for me to know.
Q. Why did you believe it was impossible for you to know whether you were responsible for the copyright infringement that occurred through your parents' Internet account?
. . .
A. Because it exceeded my capabilities as a human being.

Tenenbaum depo. at 28:5 – 30:22.

The deposition transcript is replete with similarly evasive and philosophical responses. As Defendant provided inconsistent answers and evaded questions, his claim of being forthcoming in discovery is, at best, insincere. To the extent the Court considers Defendant's conduct in discovery, this factor weighs heavily in Plaintiffs' favor.

III. PLAINTIFFS' PROPOSED METHOD OF INSPECTION IS APPROPRIATE.

To locate all the relevant and responsive information on Defendant's hard drive pertaining to Plaintiffs' claims, the contents of the hard drive must be forensically inspected. As described in the attached Declaration of Dr. Douglas Jacobson, a highly regarded professor of computer science, it is simply not possible, as a technical matter, to conduct a forensic inspection without imaging the entire hard drive.

A. Relevant Information May Be Located Anywhere on the Hard Drive.

Relevant evidence can be found in many places on a hard drive. *See* Jacobson Decl., Exhibit F. Many of these areas may not be readily viewable to the average user and therefore require a computer forensic expert to locate all relevant and responsive material. *See id.* Further, not all parts of a file will be located in the same area of the hard drive. Because computers save material in various locations and because users are able to save or move materials to various locations on a hard drive, it is impossible for Plaintiffs to specify in advance the locations where relevant data may be found on the Gateway computer's hard drive.

Moreover, computer files are not stored in a readable language but instead in magnetic binary form that must be translated using special forensic tools. *See generally,* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Civil Litigation: Is Rule 34 Up to the Task*, 41 B.C. L. Rev. 327 (2000). Thus, a forensic expert utilizing specialized tools and methods is necessary to locate files stored in any location on a hard drive. *See* Jacobson Decl., Exhibit F.

Additionally, Internet activity leaves electronic records on the hard drive. *Id.* This data, which tracks, for example, downloading and file-sharing activity via the Internet, is only accessible by a forensic computer expert. *Id.* The forensic computer expert uses specialized tools to translate the data into usable form. *Id.* Similarly, a forensic examination may also reveal any attempts to conceal evidence of infringing behavior. *See Kucala Enters., Ltd. v. Auto Wax*

Co., 2003 U.S. Dist. LEXIS 8833 (N.D. Ill. May 23, 2003). However, a forensic inspection of the entire hard drive, or the mirror image, is necessary to locate this evidence. *See* Jacobson Decl., Exhibit F. Thus, Defendant's suggestion that only specific portions of the hard drive be imaged is simply not a viable alternative.

B. Mirror Image of the Hard Drive Provides the Most Reliable Method of Inspection Without Unduly Burdening Defendant.

Discovery is considered unduly burdensome only when it outweighs its likely benefit, taking into consideration the case's needs, the amount in controversy, the parties' resources, the importance of the issues to the litigation, and the importance of the proposed discovery to resolving the issues. *Zubalake*, 217 F.R.D. at 318. The importance of a forensic examination of Defendant's computer to this case cannot be overstated. While Defendant admitted using KaZaA and LimeWire to download sound recordings from the Internet, he claimed to not remember the specifics. Evidence likely on Defendant's Gateway computer of the sound recordings at issue or use of a subsequently downloaded P2P system to upload and download sound recordings, therefore, is critical to this case.

Further, copying a hard drive using the industry-accepted method known as bit-stream imaging process, also know as mirror imaging, is the most reliable and accurate method of ensuring that the copy is an absolute duplicate in all ways of the data, in whatever form, that is on the original hard drive. *Triumph Capital Group,* 211 F.R.D. at, 48. Creating a mirror image is routine and central to a computer investigation for forensic experts. *See id.* Mirror imaging is the method utilized by law enforcement for investigating criminal matters involving computer hard drives.

The process of creating a mirror image is straightforward. The forensic technician connects the original hard drive to a special device that is also connected to another hard drive

that has previously been wiped clean so no residual data exists. *See* Jacobson Decl., Exhibit F. The mirror-imaging device then duplicates, sector by sector, exactly what is on the original drive and places it exactly the same place on the mirror image drive. *See id.* The duplication process creates a digital fingerprint, called a hash code signature ("hash code"), to verify that both drives are exactly identical in every way. This hash code is recorded. If just one character changes on the hard drive, the hash code would be different. By the use of this hash code, the mirror image drive can be verified at any point to ensure it remains exactly the same as the original drive on the date of the mirror image.

Depending on the size of the original hard drive, a mirror image may be created in just hours. The mirror imaging process does not analyze any data, it makes a perfect copy of the original hard drive. *See id.* The original can then be returned and used by the owner, and the mirror image can then be inspected for relevant and responsive files and data. *See id.*

Using a forensic expert to create and forensically examine a mirror image is not inexpensive. However, Plaintiffs are absorbing this entire cost at this stage of the proceedings. All Defendant needs to do is make his computer available for a short time and search his computer for privileged and confidential files. Contrary to Defendant's apparent misunderstanding of the mirror imaging process, he does not need a mirror imaged copy of the hard drive to conduct privilege review. This is because he is in possession of the original hard drive. Defendant can simply use his Gateway computer to search for privileged and confidential documents or information on the hard drive and create a log of these files. As these are Defendant's files, he should know better than anyone where on the Gateway computer they are stored and should be able to create a log with little to no burden to himself.

If Defendant requests a copy of the imaged hard drive, Plaintiffs will provide one at cost. The copied hard drive, however, will be formatted and therefore useless to Defendant unless he has access to an expert or technician with the proprietary software necessary to read the encoded hard drive. Jacobson Decl., Exhibit F.

The process of creating a mirror image provides a perfect duplicate for inspection and creates a method of verification that nothing on the mirror image is altered at a later date, without burdening Defendant.

IV. PLAINTIFFS ARE WILLING TO AGREE THAT NON-RELEVANT MATERIAL WILL BE PROTECTED FROM DISCLOSURE UNLESS OTHERWISE REQUIRED BY LAW.

Plaintiffs have no interest in Defendant's privileged and confidential files to the extent that they do not contain evidence relevant to the case. To make a forensically sound duplicate, however, the entire hard drive must be copied. As set forth in the proposed Protective Order (Ex. A), Plaintiffs and their expert are willing to agree to be bound by a protective order that will ensure that they will not disclose to others any non-relevant materials that may be found on Defendant's hard drive.[7] Additionally, the proposed Protective Order provides for the redaction of attorney-client privileged information or documents before the mirror image is turned over to Plaintiffs or their expert. Similarly, Plaintiffs agree to a limited redaction of confidential information such as student grades, unpublished research, and medical records. The proposed protective order contains the requisite terms and limitations and is a proper mechanism for

[7] Plaintiffs believe that most of Defendant's concerns regarding confidential information have been alleviated by limiting their request to the Gateway computer. Much of Defendant's expressed concern regarding confidentiality centered around Defendant's students' grades and unpublished research. *See* Burton Decl., ¶ 4, Ex. B Plaintiffs believe much of this information is located on Defendant's Toshiba laptop that Defendant got as a graduate student, as opposed to the Gateway computer he used in college. Thus, most of Defendant's concerns regarding confidentiality have been alleviated. Nonetheless, Plaintiffs are prepared to maintain the Gateway computer's hard drive as confidential, pursuant to the proposed protective order.

permitting the discovery permitted under the Federal Rules of Civil Procedure and protecting any non-relevant material from disclosure.

CONCLUSION

Defendant's Motion should be denied because the requested inspection seeks evidence central to Plaintiffs' claims and because such inspections are routinely allowed where, as here, the computer goes to the heart of the claim. Moreover, the requested inspection is the most appropriate and reliable method for obtaining the evidence, imposes little to no burden on Defendant, and offers ample protection for any privileged or confidential documents.

Respectfully submitted,

/s/ Eve G. Burton
Eve G. Burton
Holme Roberts & Owen LLP
1700 Lincoln Street, Suite 4100
Denver, Colorado 80203
Email: eve.burton@hro.com
Telephone: 303-861-7000

ATTORNEYS FOR PLAINTIFFS

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 30th day of October, 2008, a true and correct copy of the foregoing **Plaintiffs' Response to Defendant's Motion for Protective Order** was served email, as follows:

Charles Nesson
1575 Massachusetts Ave.
Cambridge, MA 02138
Nesson@gmail.com
Attorney for Defendant

s/ Laurie J. Rust